

УДК 004.056

Пфо О.М.

Кіровоградський національний технічний університет

## Аналіз кіберзлочинності як комплексної проблеми

Термін «кіберзлочинність» в офіційних нормативно-правових документах не визначений. Разом з тим, саме поняття закріпилося в лексиконі правоохоронних органів розвинених держав Європи і світу і має на увазі злочинність у сфері комп'ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливим постає питання модернізувати існуючі засоби захисту та розробляти і впроваджувати нові. У ряді міжнародних документів визначено, що кіберзлочинність сьогодні загрожує не тільки національній безпеці окремих держав, а й безпеці людства та міжнародному порядку. Стурбованість міжнародного співтовариства щодо розвитку кіберзлочинності знайшла відображення, зокрема, в таких міждержавних угодах як: Бангкокська декларація з попередження злочинності та кримінального правосуддя (2005 р.), Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.), Всесвітній саміт з інформаційного суспільства та Конвенції Ради Європи «Про кіберзлочинність» (2001 р.). В цих документах йдеться мова про спільне протистояння кіберзлочинам, шляхом прийняття відповідних законодавчих актів, які не будуть суперечити ні законам окремої держави ні пунктам договорів, які ратифікувала ця держава.

Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується.

Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні», а також Розділ 16 «Злочини у сфері використання ЕОМ, систем та комп'ютерних мереж» чинного Кримінального кодексу України. 3 квітня 2003 на засіданні Верховної Ради України був прийнятий за основу проект Закону «Про внесення змін до Кримінально-процесуального кодексу України», відповідно до якого будуть розширені можливості Служби безпеки України при розслідуванні порушень в роботі автоматизованих систем. Але цього виявляється не достатньо для повного подолання кіберзлочинності в нашій країні.

Отже, проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самотійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

### Список використаних джерел

1. Кіберзлочинність можна зупинити тільки разом. // Україна:бізнес. - №5-6 від 11.02.2013.
2. Комп'ютерна злочинність - К.: Атіка, 2002.
3. Кримінальний кодекс України – К.: Атіка, 2006.

